

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

昭61-16643

⑬ Int. Cl.⁴

識別記号

庁内整理番号

⑭ 公開 昭和61年(1986)1月24日

H 04 L 9/02
H 04 K 1/00

Z-7240-5K
Z-7240-5K

審査請求 未請求 発明の数 1 (全9頁)

⑮ 発明の名称 加入者キー再生システム

⑯ 特 願 昭60-48433

⑰ 出 願 昭60(1985)3月13日

優先権主張 ⑱ 1984年3月15日 ⑲ 米国(US) ⑳ 589741

㉑ 発 明 者 カール・イー・モーグ アメリカ合衆国、カリフォルニア州 92064, ポーウェイ, ホワイトウォーター・ドライブ 13360

㉒ 出 願 人 エム/エーコム・リ アメリカ合衆国、カリフォルニア州 92121, サンディエゴ, サイエンス・パーク・ロード 3033
ボレーテッド

㉓ 代 理 人 弁理士 鈴江 武彦 外2名

NO
ENGLISH
ABSTRACT

明 細 書

1. 発明の名称

加入者キー再生システム

2. 特許請求の範囲

(1) ディスクランブラに固有であると共に、エンコードキー信号、キー生成ナンバーおよび上記ディスクランブラに含まれるメモリの所定の領域をアクセスするアドレスと共に上記ディスクランブラによって受信されるスクランブル信号のディスクランブラリング用としてデコードすべきキー信号のエンコード時に使用される加入者キー信号を上記ディスクランブラで再生するシステムであって、

上記ディスクランブラに固有な加入者キー生成信号を供給する手段と、

上記ディスクランブラに固有な指定された加入者キーシード信号によってキーイングされるアルゴリズムに基く所定のエンコードアルゴリズムに従って上記加入者キー生成信号を処理することによって、上記固有の加入者キー信号を再

生する加入者キー生成器と、

上記指定された加入者キーシード信号を格納し、且つ上記指定されたシード信号を含む領域が上記キー生成ナンバーと共に受信される上記アドレスによってアクセスされたとき上記アルゴリズムをキーするために上記指定されたシード信号を供給する第1のメモリと、

上記キー生成ナンバーと共に受信される上記アドレスをもって上記第1のメモリをアクセスする手段とを具備してなる加入者キー再生システム。

(2) 上記第1のメモリが上記キー生成ナンバーと共に受信される上記アドレスに従って上記アルゴリズムをキーするために供給されている上記シード信号のうちの指定された一つを伴う複数の異なる加入者キーシード信号を格納する特許請求の範囲第1項に記載の加入者キー再生システム。

(3) 上記加入者キー生成信号を供給する手段が上記ディスクランブラに固有な加入者アドレ

ス信号を格納する第2のメモリと、上記格納された加入者アドレス信号と上記加入者キー生成信号を供給するために受信される上記キー生成ナンバーとを結合させる手段とからなる特許請求の範囲第1項記載の加入者キー再生システム。

3. 発明の詳細な説明

〔発明の技術分野〕

この発明は一般にエンコードテクノロジーに利用される通信信号スクランプリングおよびディスクランプリングシステムに係り、特にディスクランプリングに固有であると共にディスクランプリングによって受信された信号のディスクランプリング用としてデコードすべきキー信号のエンコーディング時に使用されているキー信号をディスクランプリングで再生するシステムを志向している。

〔発明の技術的背景およびその問題点〕

従来、デコードすべきキー信号のエンコーディング時に使用される上記固有のキー信号はディスクランプリングに含まれているメモリに格納さ

りに格納されてしまうからである。

この問題に対する一つの解決は例えば、固有のディスクランプリングの加入者キー信号を格納する各ディスクランプリングに安全なメモリを使用するもので、上記米国特許出願第498,800によって示唆されている。安全なメモリは集積回路化マイクロプロセッサチップ中の内部的なリードオンリメモリ(ROM)であり、このチップはチップの読み取りからROMを予防する内部アーキテクチャを有しているものとする。この安全なメモリへのアプローチはかかるディスクランプリングの固有な加入者キー信号を確認するディスクランプリングの所有者に対して高レベルの安全性を与える。

〔発明の目的〕

この発明の目的は許可されない確認およびキー信号の使用の可能性をさらに少なくし得るようディスクランプリングにおける固有な加入者キー信号の再生を複雑にすることにある。

この発明の別の目的は個々の加入者および個

れ、そしてディスクランプリングに指定された受信エンコードキー信号のデコード用メモリからアクセスされる。一般的に、ディスクランプリングの所有者はメモリからそれを読み取ることによって固有のキー信号を確認することができる。しかるに実際には、ディスクランプリングの所有者によって確認される固有のキー信号は重要な問題を提示する。例えばそれはテレビジョン予約サービスの加入者に対するスクランブルテレビジョン信号の分配制御用のキー信号エンコードテクニックに使用されるもので、米国特許出願第498,800に示されている。つまり、料金支払い済みの加入者に固有なキー信号のみが上述の分配制御に与えるものであるが、それはみかけ上である。何故なら、料金支払い済みの加入者が自分のディスクランプリングのメモリに格納されている自分の固有な加入者キー信号を確認することができるのであれば、かかる固有の加入者キー信号はスクランブルテレビジョン信号の、剽窃を可能とする不許可のディスクランプリングのメモ

個の放送者の双方に固有な加入者キー信号を使用して共通加入者通信ネットワークに有用とする複数の放送者にとって実質的な対処をなさしめる如く加入者キー信号の再生を複雑にすることにある。

〔発明の概要〕

この発明は、ディスクランプリングに固有であると共にディスクランプリングによって受信された信号のディスクランプリング用としてデコードすべきキー信号のエンコーディング時に使用されている加入者キー信号を加入者通信ネットワークのディスクランプリングで再生するシステムである。

この発明によると、スクランブル信号はエンコードキー信号、キー生成ナンバーおよびディスクランプリングに含まれるメモリの所定の領域をアクセスするアドレスと一緒にディスクランプリングによって受信される。上記スクランブル信号が上記エンコードキー信号およびキー生成ナンバーと共に受信されるという言い方は必ずしも

これらの信号が一時的に一緒に受信されるということの意味するものでなく、むしろ全てがディスクランブラによって受信されるという方がよい。実際、一般的に所定のスクランブル信号のディスクランプリング用のエンコードキー信号は所定のスクランブル信号の送信および受信の前にディスクランブラに送信され且つ受信される。

この発明のシステムはディスクランブラに固有な加入者キー生成信号を供給する手段と、ディスクランブラに固有な指定された加入者キーシード信号によってキーイングされるアルゴリズムに基く所定のエンコードアルゴリズムに従って加入者キー生成信号を処理することによって固有の加入者キー信号を再生する加入者キー生成器と、指定された加入者キーシード信号を格納し且つ指定されたシード信号を含む領域がキー生成ナンバーと共に受信されるアドレスによってアクセスされたときアルゴリズムをキーするために指定されたシード信号を供給する第

1のメモリと、キー生成ナンバーと共に受信されるアドレスでもって第1のメモリをアクセスする手段とを含んでいる。好ましくは第1のメモリは安全メモリである。

この発明のシステムは特に、複数の加入者のそれぞれに対して固有にエンコードされ、且つスクランブル信号のディスクランプリングに使用するために各加入者に固有な加入者キー信号の使用によってデコードすべき共通のキー信号をとる加入者通信ネットワークに有用である。

この発明のシステムはまた特に、複数の異なるスクランブル信号放送者によって加入者に対し固有にエンコードされ、且つスクランブル信号のディスクランプリングに使用するために加入者および放送者の双方に固有な加入者キー信号を使用することによってデコードすべき共通のキー信号をとる加入者通信ネットワークに有用であり、ここで加入者は固有にエンコードされたキー信号をデコードするために所定の放送者に固有な加入者キー信号を使用することによ

って所定の放送者からのスクランブル信号を個別にディスクランプリングするディスクランブラを有している。

好ましくは上記第1のメモリは、キー生成ナンバーと共に受信されるアドレスに従ってアルゴリズムをキーするために供給されている上記シード信号のうちの指定された一つを伴う複数の異なる加入者キーシード信号を格納する。所定の放送者によって使用されている現行の加入者キー信号のリストが知られた事実となったら、放送者はキー生成ナンバーを変更するかまたは加入者ネットワークの各ディスクランブラの第1メモリから異なる加入者キーシード信号をアクセスするアドレスを変更すればよく、その結果として加入者キー信号の完全に異なるリストがネットワークに適用可能とし得る。

システムをさらに複雑にするには、ディスクランブラ内で加入者キー生成信号を供給する手段の好ましい実施例が、ディスクランブラに固有な加入者アドレス信号を格納する第2のメモ

リと、上記格納された加入者アドレス信号と上記加入者キー生成信号とを結合する回路とを含んでいればよい。

このテクニックは共通加入者通信ネットワークを利用する異なる放送者に対して固有なキー生成ナンバーを可能とするので、異なる固有の加入者キー信号が異なる放送者によって送出されるスクランブル信号を各別にディスクランプリングする使用のために所定のディスクランブラで再生される。また、各放送者は共通グループの加入者に対して共通キー生成ナンバーを送出することを可能とする。

〔発明の実施例〕

先ず、この発明の前提となる上述した米国特許出願第498,800に開示された内容について説明すると、全体的なスクランプリングおよびディスクランプリングのうちのスクランプリング部分において、テレビジョン信号はスクランブラキー分配システムによって生成されるキーストリームでもって映像および音声部分を処理す

ることによってスクランブルされる。このスクランブラーキー分配システムはコントロールコンピュータによって供給されるチャンネルキー信号によってキーイングされたアルゴリズムに基づくデータエンスコードスタンダード(DES)アルゴリズムによってキーストリームを生成する。チャンネルキー信号はテレビジョン信号をディスクランブルするディスクランブラに必要となる。このテレビジョン信号の許可されないディスクランプリングを防止するために、チャンネルキー信号はスクランブルテレビジョン信号をスクランブルすることを許可された加入者のグループに共通のカテゴリキー信号によってキーイングされたアルゴリズムに基づくDESアルゴリズムによってエンコードされる。エンコードされたチャンネルキー信号はスクランブル信号プロセッサによってスクランブルテレビジョン信号に挿入された後、加入者ネットワークのディスクランブラに送出される。

上記カテゴリキー信号もまたエンコードされ

ることになるが、このカテゴリキーは加入者ネットワークの異なるディスクランブラにそれぞれ固有な加入者キー信号の各グループによってキーイングされるアルゴリズムに基づいたDESアルゴリズムによって固有にエンコードされる。この固有にエンコードされたカテゴリキー信号はそれぞれのディスクランブラにアドレスされると共に、加入者ネットワークのそれぞれのディスクランブラにそれを送出するスクランブル信号プロセッサによってスクランブルテレビジョン信号に挿入される。

上記固有な加入者キー信号のリスティングは加入者キー分配システムによる場合を除いては利用されないように維持される。このリスティングが不許可のアクセスによって危険にさらされたら、加入者キー信号の新しいリスティングが準備され且つ利用されなければならない。上記コントロールコンピュータはまた放送者に固有なシステムキー生成ナンバーをスクランブラ信号プロセッサに供給し、このシステムキー生成ナン

バーはまた全ての加入者への送信用としてスクランブルテレビジョン信号中に挿入される。さらにスクランブラ信号処理器はスクランブルテレビジョン信号中にコントロールコンピュータによって供給されたプロセスコントロール信号および初期化ベクトル(IV)フレームカウント信号を挿入する。

上記スクランブルテレビジョン信号をディスクランブルするために各ディスクランブラにおいては、テレビジョン信号をスクランブルするのには、使用されたキーストリームが再生されなければならない。ディスクランブラでキーストリームを再生するためには、エンコードチャンネルキー信号がスクランブラのキーストリームを生成するのに使用されたチャンネルキーを再生するためにデコードされなければならない。所定のディスクランブラにおけるエンコードチャンネルキー信号をデコードするためには、所定のディスクランブラに対してアドレスされた固有のエンコードカテゴリキーがスクランブラにおい

てチャンネルキー信号をエンコードするのに使用されたカテゴリキー信号を再生するのにデコードされなければならない。所定のディスクランブラにおける固有のエンコードカテゴリキー信号をデコードするためには、スクランブラにおいてカテゴリキー信号をエンコードするのに使用された固有の加入者キー信号がそのディスクランブラにおいて再生されなければならない。

第1図を参照すると、ディスクランブラはディスクランブラ信号プロセッサ150およびディスクランブラキー分配システム151とを含んでいる。

このディスクランブラ信号プロセッサ150はライン152のスクランブルテレビジョン信号を受信する。ディスクランブラ信号プロセッサ150は上記受信したスクランブルテレビジョン信号からディスクランブラキー分配システム151の動作に関係するIVフレームカウント信号(図示せず)エンコードチャンネルおよびエンコードカテゴリキー信号(ライン156)、加入

者キー生成ナンバー(ライン157)および種々のプロセスコントロール信号(ライン158)を分離してディスクランブラーキー分配システム151に供給する。

このディスクランブラーキー分配システム151はライン152で受信したスクランブルテレビジョン信号の映像および音声成分をスクランブルするのに使用された固有のキーストリームを再生することによって信号プロセッサからライン156~158を介して受信されたそれらの信号に回答し、ライン159を介してディスクランブラ信号プロセッサ150に固有のキーストリームを供給する。

ディスクランブラ信号プロセッサ150はライン160にディスクランブルされた映像信号を且つライン161にディスクランブルされた音声信号を供給するために、ライン159で受信された固有のキーストリームに従ってライン152のスクランブルテレビジョン信号をディスクランブルする。

固有な加入者キーシード信号によってキーイングされたDESアルゴリズムによるDESエンコードアルゴリズムに従ってライン180の加入者キー生成信号を処理することにより、ライン181に固有な64ビットの加入者キー信号を生成する。ライン181の固有な加入者キー信号のうちの8ビットは、ディスクランブラにアドレスされた固有なエンコードカテゴリキー信号の生成をキーするのにスクランブラにおいて使用されている固有な56ビット加入者キー信号を再生するために切り捨て機能素子166によって取り除かれる。

安全メモリ163からライン179に引き出された加入者キーシード信号の内容に基づいて加入者キー生成器165によりライン181に生成された加入者キー信号の内容が重要である故に、ディスクランブラにアドレスされた固有のエンコードカテゴリキー信号の生成をキーするのにスクランブラにおいて使用されたそれと全く同一の固有な加入者キー信号の生成をキーす

第2図を参照すると、第1図のディスクランブラキー分配システムシステム151において使用される加入者キー再生システムの一つの好ましい実施例は、4つの加入者キーシード信号を格納する安全な加入者キーシードメモリ163と、ディスクランブラに固有な加入者アドレス信号を格納する加入者アドレスメモリ164と、加入者キー信号生成器165とを含んでいる。

上記メモリ163は格納されている4つの固有な加入者キーシード56ビット信号をライン179に供給するために、ライン167で受信された32ビットシステムキー生成ナンバーの所定の位置に含まれている2ビットによりライン298を介してアドレスされる。

メモリ164に格納されている32ビットの固有な加入者アドレス信号は、ライン180に64ビットの加入者キー生成信号を供給するために、ライン157で受信された32ビットシステムキー生成ナンバーと結合される。

加入者キー生成器165は、ライン179の

ることになる加入者キーシード信号に含まれている安全メモリ163のロケーションをシステムキー生成ナンバーにおける2つのアドレスビットがアドレスする。

ディスクランブラキー分配システム151はさらにカテゴリキー生成器167を含んでいる。このカテゴリキー生成器167はライン156にアドレスされた固有なエンコードカテゴリ信号を受信し、そしてライン182に固有の加入者キー信号が再生されたとき、ライン182の固有な加入者キー信号によってキーイングされたDESアルゴリズムに基づくDESエンコードアルゴリズムに従ってライン156を介して受信されたエンコードカテゴリキー信号を処理することにより、ライン183にデコードされた64ビットのカテゴリキー信号を生成する。

図示しないキーストリーム生成器を除いて、第1図のディスクランブラキー分配システム151の構成要素は全てシングルマイクロプロセッサチップに含まれるものとし、具体的には

例えばインテル社製8751シングルコンポーネント8ビットマイクロコンピュータのスペシャルバージョンでよい。インテル社製8751に代るものとしては同一性能を与えるテキサスインスツルメンツ社製TMS7041とTMS70C40との組合せがある。インテル社製“8751”チップはHMOSテクノロジーで製作されたスタンドアロン、ハイパフォーマンス、シングルチップのコンピュータであって、40ピンDIPにパッケージされている。それはこの種の暗号法の応用における効果的なコントローラとして必要なハードウェア上の特徴、アーキテクチャルエンハンスメントおよびインストラクションセットを提供する。このスペシャルバージョンの8751チップのEPROMはチップに読み出すのみの4KバイトのUV消去リードオンリメモリを含んでいる。アーキテクチャは製造プロセスにおいて“ペリファイモード”のヒューズをとばすことによって外部ペリファイモードが不能になされているならば、EPROMからチップの外側に向う通路

をいささかとも提供しない。全てのファームウェアはこのEPROM領域に含まれるキー信号の生成およびストレージを遂行する。8751チップの安全なEPROMに格納されたプログラムを読み出すことの極度の困難さは加入者キー信号および加入者アドレスのリストの使用をなすための剽窃にとってはおろか多くの困難をもたらす。これは、たとえ剽窃者がそのリストを得るのにコントロールコンピュータの安全システムの破壊に成功したとしてもである。若し、剽窃者が確かな加入者キー信号を知っていたとしても、その者はその者がメモリ中に確かな加入者キー信号シードおよび加入者アドレスを格納し得る全体のプログラムを知らなければならない。これは製造者のセキュリティ手続きによって保護される完全なプログラムリストなしでするのは極めて困難である。

第3図および第4図に示される好ましい実施例における固有な加入者キー信号の再生は2つの異なるキーシード信号を実用化することによ

ってさらに複雑となっている。

第3図の実施例は加入者キーシードメモリ163、加入者アドレスメモリ164および第2図の実施例に含まれている加入者キー生成器165を含むと共に、さらに第2のキー生成器300を含んでいる。

メモリ163は、格納された4つの固有な加入者の56ビットキーシード信号の第1指定部をライン179に供給するために、ライン157で受信された32ビットのシステムキー生成ナンバーの第1の所定位置に含まれている2ビットによってライン298を介してアドレスされると共に、格納された4つの固有な加入者キーシード信号の異なる第2指定部をライン301に供給するために、ライン157で受信されたシステムキー生成ナンバーの第2の所定位置に含まれている2ビットによってさらにアドレスされる。

メモリ164に格納されている32ビットの固有な加入者アドレス信号は、ライン302に

64ビットの第2のキー生成信号を供給するためにライン157で受信された32ビットの加入者キー生成ナンバーに結合される。

第2のキー生成器300は、ライン301の第2指定部の固有な加入者キーシード信号によってキーイングされるDESアルゴリズムに基づくDEPエンコードアルゴリズムに従ってライン302の第2のキー生成信号を処理することによってライン303に64ビットの固有な加入者キー生成信号を生成する。

加入者キー生成器165は、ライン179の第1指定部の固有な加入者キーシード信号によってキーイングされるDESアルゴリズムに基づくDESエンコードアルゴリズムに従ってライン303の加入者キー生成信号を処理することによってライン181に64ビットの固有な加入者キー信号を生成する。ライン181の固有な加入者キー信号のうちの8ビットはディスクランブラにアドレスされた固有なエンコードカテゴリキー信号の生成をキーするのにスクランブ

ラにおいて使用されている固有な加入者キー信号と全く同一の固有な56ビットの加入者キー信号をライン182に供給するために切り捨て機能素子166によって取り除かれる。第3図のシステムのこの他の全ての態様は第2図のシステムと同じである。

第4図の実施例は加入者キーシードメモリ163, 加入者アドレスメモリ164, 加入者キー生成器165および第3図の実施例に含まれている第2のキー生成器300を含むと共に、さらに第3のキー生成器306を含んでいる。

メモリ163は、格納されている4つの固有な加入者56ビットキーシード信号の第1指定部をライン179に供給するのに、ライン157で受信された32ビットのシステムキー生成ナンバーの第1の所定位置に含まれる2ビットによってライン298を介してアドレスされると共に、さらに格納されている4つの固有な加入者キーシード信号のうちの異なる第2指定部をライン301に供給するのに、ライン157で

受信されたシステムキー生成ナンバーの第2の所定位置に含まれる2ビットによってアドレスされる。

メモリ164に格納されている32ビットの固有な加入者アドレス信号は、ライン306に64ビットの第3のキー生成信号を供給するのにライン157で受信された32ビットの加入者キー生成ナンバーと結合される。

第3のキー生成器306は、ライン179の第1指定部の固有な加入者キーシード信号によってキーイングされるDESアルゴリズムに基づくDESエンコードアルゴリズムに従ってライン306の第3のキー生成信号を処理することによってライン307に64ビットの固有な第2のキー生成信号を生成する。

第2のキー生成器300は、ライン301の第2指定部の固有な加入者キーシード信号をDESアルゴリズムに基づくDESエンコードアルゴリズムに従ってライン307の第2のキー生成信号を処理することによってライン303に

64ビットの固有な加入者キー信号を生成する。

加入者キー生成器165は、ライン179の第1指定部の固有な加入者キーシード信号によってキーイングされるDESアルゴリズムに基づくDESエンコードアルゴリズムに従ってライン303の加入者キー生成信号を処理することによってライン181に64ビットの固有な加入者キー信号を生成する。ライン181の固有な加入者キー信号のうちの8ビットはディスクランブラにアドレスされた固有なエンコードカテゴリキー信号の生成をキーするのにスクランブラにおいて使用されている固有な加入者キー信号と全く同一の固有な56ビットの加入者キー信号をライン182に供給するために切り捨て機能素子166によって取り除かれている。第4図のシステムのこの他の態様は第2図のシステムと同じである。

〔発明の効果〕

上述したところから明らかであるように、この発明の加入者キー再生システムは多くの有利

な特徴を有している。

1つの特徴は再生される固有な加入者キー信号をスクランブラのコントロールコンピュータによって供給されると共にディスクランブラに送出するためのスクランブルド信号に挿入されるシステムキー生成ナンバーを変更することによって簡単に変更することができるということである。

別の特徴は所定の加入者通信ネットワーク用の固有な加入者キー信号の異なるセットは異なる放送者による使用のために生成することができるということであり、これによって異なる放送者からのスクランブルド信号は同じディスクランブラによって固別的にディスクランブルすることができる。従って、このシステムを使用する各放送者は他の放送者のリスティングの機密性を危険にさらすことなく、固有の加入者キー信号そのものの独立したリスティングを準備することができる。

付加的な特徴は、ディスクランブラのメモリ

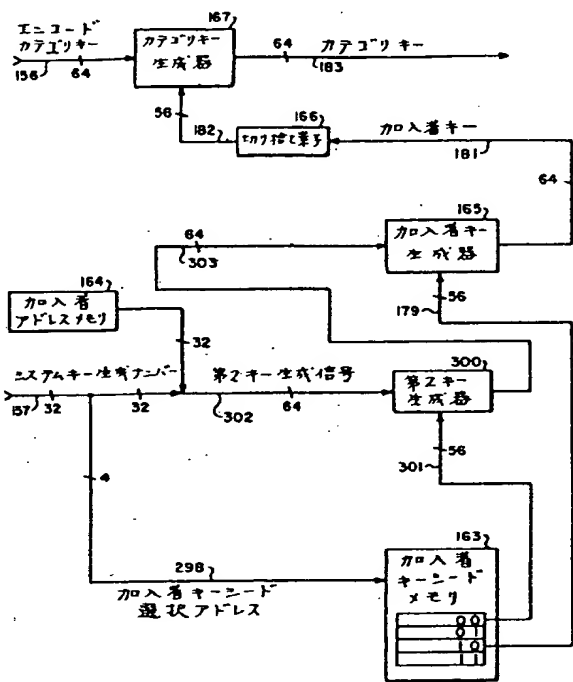


FIG 3

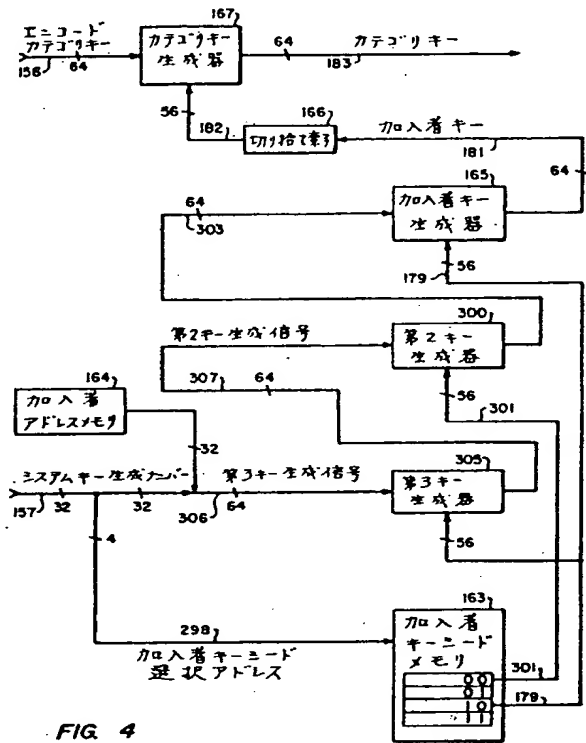


FIG 4